(19) JAPANESE PATENT OFFICE (JP)

(12) KOKAI TOKUHYO PATENT GAZETTE (A)

(11) PATENT APPLICATION PUBLICATION NO. P2000-514625A
(43) Publication Date: October 31, 2000

(51) Int. Cl.[7]:	Identification Codes:	FI	Theme Codes (for reference)
H 04 Q 7/38		H 04 B 7/26	109R
G 09 C 1/00	640	G 09 C 1/00	640D
H 04 L 9/32		H 04 L 9/00	675A
			673E

Examination Request: Not filed Preparatory Examination: Requested (Total of 46 pages)

(21) Filing No.:	Hei 10[1998]-505687	(71) Applicant:	Gemplus S.C.A Parc d'activités de Gemenos, Avenue du Pic-de-Bertagne, Gemenos Cedex F-13881, France
(86) (22) Filing Date:	July 11, 1997		
(85) Translation Filing Date:	January 11, 1999		
(86) International Application Date:	PCT/FR97/01298		
(87) International Publication No.:	WO98/03026	(72) Inventor:	Philippe Proust 1 Avenue Canté Coucou, La Ciotat, F-13600 France
(87) International Publication Date:	January 22, 1998		
(31) Priority No.:	96/08906	(72) Inventor:	Anne Laget 6 Rotisman Rue Le Ward, Route de Solan, Aubagne, F-13400 France
(32) Priority Date:	July 11, 1996		
(33) Priority Country:	FR		
(81) Designated States:	EP (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), AU, CA, CN, JP, US	(74) Agent:	Keiichi Ota, patent attorney

Continued on last page

(54) [Title] ENHANCED SHORT MESSAGE AND METHOD FOR SYNCHRONIZING AND ENSURING SECURITY OF ENHANCED SHORT MESSAGES EXCHANGED IN A CELLULAR RADIO COMMUNICATION SYSTEM

(57) Abstract

The present invention pertains to a prescribed structure for enhanced messages and to a method for synchronizing and ensuring the security of exchanging enhanced messages having the aforementioned structure. Conventionally, an enhanced message is sent to a subscriber identity module (or SIM) of a mobile station by a message service center. The main body (2) of the enhanced message has a first field (3) for storing remote commands pertaining to a remote application. According to the present invention, said main body (2) also has a second field (4) that stores the current value of a synchronization counter to be compared with the previous value of the synchronization counter stored in the SIM. According to the present invention, main body (2) can also have another field (6) that stores a certificate, the signature of the main body for certifying the authenticity of the enhanced message and the identity of the sender. The enhanced message is accepted or rejected by the SIM corresponding to the consistency of these values with the internal state of the SIM.

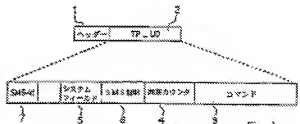

Fig. 1

Key: 1 Header
3 Command
4 Synchronization counter
5 System field
6 SMS certificate

Claims

1. An enhanced message of the type transmitted by a message service center (C-SMS) to a mobile station (MS) in a cellular radio communication system and having a header (1) and a main body (2), with said main body (2) particularly having a first field (3) for storing the remote commands pertaining to a remote application of the aforementioned mobile station;

said mobile station being constituted with a terminal cooperating with a subscriber identity module, said terminal having a means for receiving said enhanced message, said subscriber identity module having a means for storing and processing the received enhanced message, and said subscriber identity module having a means for executing said remote commands to support said remote application;

said enhanced message being characterized by the fact that said main body (2) also has a second field (4) for storing the current value of a synchronization counter;

the current value of the synchronization counter being compared with the previous value of the synchronization counter stored in the subscriber identity module so that said enhanced message is accepted or rejected by the subscriber identity module corresponding to the result of comparing the current value and the previous value of the synchronization counter, and said previous value being updated by said current value only when the enhanced message is accepted by the subscriber identity module.

2. The enhanced message described in Claim 1, characterized by the fact that the main body (2) of said enhanced message also has a third field (5) for storing a first piece of locating information indicating the location in said data storage means of the subscriber identity module where said previous value of the synchronization counter is stored.

3. The enhanced message described in Claim 2, the data storage means of the subscriber identity module having a hierarchical structure of at least three levels and having at least the following three kinds of files:

• master file (MF), or primary directory;

• dedicated file (DF) or secondary directory located under said master file;

• elementary file (EF) located under said dedicated file known as parent dedicated file or directly located under said master file known as parent master file;

an elementary system file (EF SMS System) suitable for said remote application having a second piece of locating information indicating the location in the data storage means of the subscriber identity module where said previous value of the synchronization counter is stored;

characterized by the fact that the first piece of locating information stored in said third field (5) is an identifier for dedicated file (DF) or master file (MF) related to said elementary system file (EF SMS System) depending on a predetermined search strategy in the data storage means.

4. The enhanced message described in any of Claims 1-3, characterized by the following facts: said main body also has a fourth field (6) for storing ciphertext known as transmitted ciphertext, calculation of which at least partially includes the content of the second field storing the current value of the synchronization counter;

said transmitted ciphertext is compared with another ciphertext known as local ciphertext as calculated by the subscriber identity module such that said enhanced message is accepted by the subscriber identity module if the transmitted ciphertext is the same as the local ciphertext and is rejected otherwise.

5. The enhanced message described in Claim 4, characterized by the fact that calculation of said transmitted and local ciphertext at least partially includes the content of the first field (3) storing the remote commands.

6. The enhanced message described in Claim 5, characterized by the fact that calculation of said transmitted and local ciphertext at least includes all the content of the second field (4) storing the current value of the synchronization counter and all the content of the first field (3) storing the remote commands.

7. The enhanced message described in any of Claims 1-6, characterized by the fact that

said transmitted and local ciphertext are calculated by using a cryptographic function belonging to the group of

• secret key cryptographic functions; and

• public key cryptographic functions.

8. The enhanced message described in any of Claims 1-7, said subscriber identity module storing a cryptographic function and an associated key specific to said remote application in the data storage means of the subscriber identity module to calculate said local ciphertext, characterized by the fact that the main body of said enhanced message also has a fifth field (5) storing a third piece of locating information indicating the location in said data storage means where said cryptographic function and said associated key specific to said remote application are stored.

9. The enhanced message described in Claim 2 or 8, characterized by the fact that said third field (5) also constitutes said fifth field, and said first piece of locating information also constitutes said first piece of locating information.

10. The enhanced message described in any of Claims 1-9, said main body also having a sixth field (7) storing a checksum known as transmitted checksum, calculation of which at least partially includes the content of the first field (3) storing remote commands,

characterized by the fact that said transmitted checksum is compared with another checksum known as local calculation total calculated by the subscriber identity module such that

said enhanced message is accepted by the subscriber identity module if the transmitted checksum is the same as the local checksum and is rejected otherwise.

11. The enhanced message described in any of Claims 1-10, characterized by the fact that said subscriber identity module has an input/output line and receives local commands belonging to a local application in said mobile station on said input/output line, and

said remote commands included in the first field (3) of said enhanced message are virtually the same as said local command received by the input/output line.

12. A method for synchronizing and ensuring security of enhanced messages exchanged between a message service center (C-SMS) and a mobile station (MS) of a cellular radio communication system, wherein each enhanced message has a header (1) and a main body (2), said main body (2) particularly has a first field (3) for storing the remote commands pertaining to a remote application of the aforementioned mobile station;

said mobile station is constituted with a terminal cooperating with a subscriber identity module, said terminal has a means for receiving said enhanced message, said subscriber identity module has a means for storing and processing the received enhanced message, and said subscriber identity module has a means for executing said remote commands to support said remote application;

said method particularly having the following steps:

• said message service center sends an enhanced message that also has a second field (4) storing the current value of a synchronization counter in the main body to said mobile station (61);

• the subscriber identity module of the mobile station compares the current value of the synchronization counter included in said enhanced message with the previous value of the synchronization counter stored in the subscriber identity module (65:85);

• the subscriber identity module accepts (67) or rejects (66) said enhanced message depending on the result of comparing the current value with the previous value of the synchronization counter;

• the subscriber identity module updates said previous value by said current value if the enhanced message is accepted (86).

13. The method described in Claim 12, characterized by the fact that the current value of the synchronization counter is incremented by a certain amount for each new enhanced message of said remote application transmitted by said message service enter, and

said enhanced message is accepted by the subscriber identity module only when the current value of said synchronization counter is larger than said previous value.

14. The method described in Claim 12 or 13, characterized by the fact that said step of updating the previous value of the synchronization counter by the current value is carried out

only when the difference between the current value and the previous value is smaller than a prescribed maximum incrementation.

15. The method described in any of Claims 12-14, characterized by also having the following step:

• if said enhanced message is rejected by the subscriber identity module (66), the subscriber identity module will send an enhanced message including a specific error code that can notify the message service center of the fact that the enhanced message it just transmitted has been rejected due to the synchronization problem of the counter to the message service center (87).

16. The method described in any of Claims 12-15, wherein the main body (2) of said enhanced message transmitted by the message service center to the mobile station also has a third field (5) storing a first piece of locating information indicating the location in said data storage means where said previous value of the synchronization counter is stored, characterized by the fact that the following steps are carried out before the subscriber identity module compares the current value and the previous value of the synchronization counter (85):

• the subscriber identity module reads the first piece of locating information stored in the third field of said enhanced message (82);

• the subscriber identity module deduces the previous value of the synchronization counter from the piece of locating information (83);

the subscriber identity module reads the previous value of the synchronization counter stored at the aforementioned location (84).

17. The method described in any of Claims 12-16, wherein said enhanced message (2) transmitted by the message service center to the mobile station also has a fourth field (6) storing a ciphertext known as transmitted ciphertext calculated by at least partially using the content of the second field (4) storing the current value of the synchronization counter,

characterized by also having the following steps:

• the subscriber identity module at least partially uses the content of the second field (4) in said enhanced message to calculate a local ciphertext (92);

• the subscriber identity module compares said transmitted ciphertext with said local ciphertext (93) such that said enhanced message is accepted if the transmitted ciphertext is the same as the local ciphertext and is rejected otherwise.

18. The method described in any of Claims 12-17, wherein said subscriber identity module stores a cryptographic function and an associated key specific to said remote application in the data storage means of the subscriber identity module to calculate said local ciphertext, and

said enhanced message transmitted by the message service center to the mobile station also has a fifth field (5) storing a third piece of locating information indicating the location in

said data storage means where said cryptographic function and said associated key specific to said remote application are stored,

characterized by the fact that the aforementioned step of calculating the local ciphertext by the subscriber identity module (92) has the following steps:

• the subscriber identity module reads said third piece of locating information stored in the fifth field (5) of said enhanced message (94);

• the subscriber identity module deduces the storage locations of said cryptographic function and said associated key from the piece of locating information;

• the subscriber identity module uses said cryptographic function and said associated key as well as at least part of the content of the second field (4) in said enhanced message to calculate said local ciphertext (96).

19. The method described in Claim 16 or 18, wherein the data storage means of the subscriber identity module has a hierarchical structure of at least three levels and having at least the following three kinds of files:

• master file (MF), or primary directory;

• dedicated file (DF) or secondary directory located under said master file;

• elementary file (EF) located under said dedicated file known as parent dedicated file or directly located under said master file known as parent master file, characterized by the following facts:

an elementary system file (EF SMS System) suitable for said remote application has a second piece of locating information indicating the location in the data storage means of the subscriber identity module where said previous value of the synchronization counter is stored;

said third field (5) also constitutes said fifth field, and said first piece of locating information also constitutes said third piece of locating information;

the first piece of locating information stored in said third field (5) is an identifier for dedicated file (DF) or master file (MF) related to said elementary system file (EF SMS System) depending on a predetermined search strategy in the data storage means.

20. The method described in any of Claims 12-19, wherein, preferably, the main body (2) of said enhanced message transmitted by the message service center to the mobile station also has a sixth field (7) storing a checksum known as transmitted checksum, calculation of which at least partially includes the content of the first field (3) storing remote commands,

characterized by also having the following steps:

• the subscriber identity module uses at least part of the content of the first field (3) in said enhanced message to calculate a local checksum (72);

• the subscriber identity module compares said transmitted checksum with said local checksum such that said enhanced message is accepted if said transmitted checksum is the same as the local checksum and is rejected otherwise (73).

Detailed explanation of the invention

Enhanced short message and method for synchronizing and ensuring security of enhanced short messages exchanged in a cellular radio communication system

The present invention belongs to the field of messages exchanged in a cellular radio communication system. In general, these messages are exchanged between a message service center and a plurality of mobile stations. Each mobile station is constituted with a terminal cooperating with a user card formed by a microprocessor known as a subscriber identity module (or SIM).

More specifically, the present invention pertains to a special structure for enhanced messages and to a method for synchronizing and ensuring the security of exchanging the enhanced messages having the aforementioned structure.

The GSM standard (global system for mobile public communications operating in the 900 MHz band) is known in the field of cellular radio communication, especially, in Europe.

The present invention is particularly applied to systems depending on said GSM standard but is not limited to that.

In general, a terminal is a physical device used by a user to access the telecommunication service provided by a network. There are various kinds of terminals, such as portable terminals, mobile terminals, and vehicle-mounted terminals.

When a user uses a terminal, he (or she) must connect a chip card type user card (SIM) of his (or her) own to the terminal.

The user card supports its own operation and a principal application (such as a GSM application) of telephone that can operate the terminal to which it is connected in a cellular radio communication system. In particular, the user card provides a unique identifier (or IMSI, "International Mobile Subscriber Identity") of the subscriber to the terminal to which it is connected.

Therefore, the user card has command execution means (such as a microprocessor and program memory) and data storage means (such as data memory).

The IMSI identifier and all of the personal information regarding the subscriber used by the terminal are stored in the data storage means of the SIM. In this way, each terminal can be used with any SIM.

In a known specific system, especially, the GSM system, there is a message service (or SMS, "Short Message Service") that can transmit messages (known as short messages in the case

of GSM) to mobile station. These messages are sent out by a message service center (or SMS-C, "SMS-Center").

When a certain mobile station receives a message, it stores the message in the data storage message of its SIM. The principal telephone application of each SIM can process the received message.

Originally, the only function of message is to provide information to a subscriber through the display screen of a terminal. Therefore, the message known as standard message used for realizing said only function only includes raw data.

Then, an enhanced message (or ESMS, "Enhanced SMS") that can send two kinds of messages, that is, the aforementioned standard message and commands, was designed.

Consequently, it has been already proposed that commands that can update or reconstruct said SIM remotely are transmitted to the SIM via enhanced message. In other words, the commands encapsulated in enhanced messages can change the principal telephone application of the SIM. In this way, it is possible to reconstruct an SIM without taking it to a retail shop (thus, management commands can be executed in the SIM when it is in the application stage).

It has also been proposed to use SIMs to support other applications, such as a rental car, payment, and loyalty applications, in addition to the principal telephone application.

Since the commands belonging to said other applications are included in the enhanced messages and are thus outside the SIM, said other applications are known as remote or OTA ("Over the Air") applications. On the other hand, the principal telephone application stored in the data storage means of the SIM is known as the local application. The commands are known as local or remote commands depending on whether an application is a local or remote application.

The remote applications (rental, payment, reconstructing the principal telephone application, etc.) can be executed in accordance with the aforementioned remote commands.

It is clear that this recent remote application concept (or OTA application) is very beneficial to the subscribers. The subscribers can carry out various applications, such as renting a car or making a payment, very easily by simply using a terminal into which the subscriber's SIM is inserted.

In other words, the SIM can execute some applications other than the application it usually carries out (that is, more commands) once it is in the application stage, that is, once it is inserted into the cellular phone of a user.

Special security is required as a result of said increase in the operation capacity of the SIM. In fact, this mechanism acting as an additional entrance gate into the SIM should be able to prevent anybody from performing any operation that is usually prohibited for that person in the SIM.

The special security requirements associated with use of enhanced message particularly include resynchronization, uniqueness of each message, integrity of each message, authenticity of the sender, and the like.

In fact, it is desired that resynchronization can be achieved between the message source and SIM when a transmission problem occurs in the network. Due to unpredictable transmission of the enhanced message channel, it is actually unable to guarantee the routing of the enhanced message or the routing order of a plurality of enhanced messages.

The requirement on the uniqueness of each message can prevent replay of message either accidentally (a transmission channel that traces enhanced message may actually send the same message several times to the same SIM) or intentionally (that is, with a purpose of fraud, for example, repeatedly executing the same sequence of commands, such as commands enabling recrediting of a prepaid telephone usage counter in the SIM, in the SIM).

The requirement on the integrity of each message can prevent modification of a message either accidentally (also depending on the transmission channel between the message service center and the mobile station) or intentionally (with the idea of modifying a message to execute other actions more sensitive than those predetermined by the message source).

The requirement on the authenticity of the sender can reliably confirm the permission of sending the enhanced message. In fact, this remote application mechanism must be specially reserved for specific senders (such as operations and service providers).

The recent remote application concept being implemented currently, however, does not meet all of the aforementioned specific security requirements.

In fact, the only scheme that has been proposed so far is to introduce a checksum into each enhanced message and run a secret code prompt type check procedure before executing the remote commands included in the enhanced message.

Clearly, this solution is incomplete and thus unsatisfactory.

First of all, the use of a checksum considered as a relatively basic solution can only ensure that the message is transmitted correctly.

Second of all, the procedure for secret code check cannot provide sufficient security guarantee if an enhanced message is intercepted. In fact, since the identification information does not vary for each message, it is easy for a person without permission to replay a message, that is, it is easy for an improperly intercepted message to pass as an authentic one.

Finally, the known solution cannot fully satisfy the aforementioned other requirements, that is, the requirements regarding resynchronization and integrity of the message.

The objective of the present invention is to solve the various problems of the conventional technology.

More specifically, one of the objectives of the present invention is to provide a method for synchronizing and ensuring security of exchange of enhanced messages and a corresponding enhanced message structure that can resynchronize the message source and the SIM when a transmission problem occurs in a network.

Another objective of the present invention is to provide an enhanced message method and structure for guaranteeing the uniqueness of each transmitted enhanced message.

Yet another objective of the present invention is to provide an enhanced message method and structure for guaranteeing the integrity of each transmitted enhanced message.

A supplementary objective of the present invention is to provide an enhanced message method and structure for guaranteeing the authenticity of the enhanced message sender.

The aforementioned various objectives and other objectives to be described later are realized by the present invention by using a type of enhanced message transmitted by a message service center to a mobile station in a cellular radio communication system. The enhanced message has a header and a main body, and said main body particularly has a first field storing remote commands belonging to a remote application of said mobile station.

Said mobile station is constituted with a terminal cooperating with a subscriber identity module. Said terminal has a means for receiving said enhanced message. Said subscriber identity module has a means for storing and processing the received enhanced message, and said subscriber identity module has a means for executing said remote commands to support said remote application.

Said enhanced message is characterized by the fact that said main body also has a second field for storing the current value of a synchronization counter.

The current value of the synchronization counter is compared with the previous value of the synchronization counter stored in the subscriber identity module so that said enhanced message is accepted or rejected by the subscriber identity module corresponding to the result of comparing the current value and the previous value of the synchronization counter, and said previous value is updated by said current value only when the enhanced message is accepted by the subscriber identity module.

In this way, synchronization between the message service center and the subscriber identity module (or SIM) is based on the use of the counter shared between them. Each message sent to the SIM includes the current value of its synchronization counter. That current value is distinguished for each message. On the other hand, the SIM stores the previous value of the synchronization counter and compares it with the current value included in each message to accept or reject the message.

If a problem occurs when transmitting a message, the SIM can be resynchronized with the message source starting from the next message. This is because the current value of the synchronization counter is included in each message.

If the SIM has a plurality of remote applications, each of them can be combined with another synchronization counter. In this case, the SIM stores the previous values of different counters.

Preferably, the main body of said enhanced message also has a third field storing a first piece of locating information indicating the location in said data storage means where said previous value of the synchronization counter is stored.

This is particularly advantageous when the SIM includes a plurality of remote applications. In this case, when a message is received, the SIM will know which synchronization counter to use depending on the content of the third field.

The data storage means of the subscriber identity module has a hierarchical structure of at least three levels and having at least the following three kinds of files:

- master file, or primary directory;
- dedicated file or secondary directory located under said master file;
- elementary file located under said dedicated file known as parent dedicated file or directly located under said master file known as parent master file.

An elementary system file (EF SMS System) suitable for said remote application has a second piece of locating information indicating the location in the data storage means of the subscriber identity module where said previous value of the synchronization counter is stored.

In this specific embodiment of the present invention, the enhanced message is characterized by the fact that the first piece of locating information stored in said third field is an identifier for the dedicated file or the master file related to said elementary system file depending on a predetermined search strategy in the data storage means.

Consequently, each message includes an identifier enabling the SIM to find the basis system file to which the remote application sends said message is linked. This basic system file particularly includes the previous value of the synchronization counter associated with the remote application that sends said message.

Preferably, said main body also includes a fourth field for storing ciphertext known as transmitted ciphertext, calculation of which at least partially includes the content of the second field storing the current value of the synchronization counter.

Said transmitted ciphertext is compared with another ciphertext known as local ciphertext as calculated by the subscriber identity module such that said enhanced message is accepted by the subscriber identity module if the transmitted ciphertext is the same as the local ciphertext and is rejected otherwise.

In other words, uses of the synchronization counter and the ciphertext are combined. In this way, the security for exchanging messages between the message service center and the SIM can be improved. The use of the ciphertext enables the SIM to confirm that the message transmission source is a truly authorized source (also known as the authenticity of the sender) and to confirm the integrity of the message.

Additionally, since calculation of the current value of the counter is included in the calculation of the ciphertext, there is synergistic effect between the use of the synchronization counter and the use of the ciphertext.

First of all, since the current value of the counter is different for each message, it is unable to replay the same message improperly. In other words, the uniqueness of each message can be guaranteed this way.

Also, since the current value of the counter is included in the message, the SIM knows which current value has been used to calculate the ciphertext so that the comparative ciphertext (local ciphertext) can be calculated on the same basis.

Finally, since the current value of the counter in the message is transmitted, even if the message transmitted previously has not been received (or has not arrived), it can guarantee that the received message will be accepted.

Advantageously, the content of the first field storing the remote commands is at least partially included in the calculation of said transmitted and check ciphertext.

According to an advantageous embodiment of the present invention, calculation of said transmitted and local ciphertext at least includes all the content of the second field storing the current value of the synchronization counter and all the content of the first field storing the remote commands. In this way, the security can be improved.

Preferably, said transmitted and local ciphertext are calculated by using a cryptographic function belonging to the group of

- secret key cryptographic functions; and
- public key cryptographic functions.

In this way, the present invention is not limited to use of a specific type of cryptographic function.

Preferably, said subscriber identity module stores a cryptographic function and an associated key specific to said remote application in the data storage means of the subscriber identity module so that it is possible to calculate said local ciphertext.

Said enhanced message is characterized by the fact that the main body of said enhanced message also has a fifth field storing a third piece of locating information indicating the location in said data storage means where said cryptographic function and said associated key specific to said remote application are stored.

This is particularly beneficiary in the case when the SIM supports a plurality of remote applications, each of which is associated with different pairs (cryptographic function, key) or in the case when the SIM stores different pairs associated with said different applications. In this case, when a certain message is received, the content of the fifth filed can be used so that the SIM knows which pair (cryptographic function, key) to use.

According to a recommended embodiment of the present invention, said third field also constitutes said fifth field, and said first piece of locating information also constitutes said third piece of locating information.

In this way, the content of the third field can tell the SIM not only which synchronization counter to use but also which pair (cryptographic function, key) to use.

Advantageously, said main body also has a sixth field storing a checksum known as transmitted checksum, calculation of which at least partially includes the content of the first field storing remote commands.

Said transmitted checksum is compared with another checksum known as a local calculation total calculated by the subscriber identity module such that said enhanced message is accepted by the subscriber identity module if the transmitted checksum is the same as the local checksum and is rejected otherwise.

An additional level of security can be constituted by using said checksum. In this way, a message modified accidentally can be quickly rejected without carrying out the cryptographic calculation.

Additionally, if the possibility of stopping the ciphertext check and the counter check under specific conditions is predicted, the "hash field" alone can guarantee that message would not be varied accidentally or intentionally although the guarantee has a very relative level. Of course, however, that possibility must be limited to a configuration in which the logic security linked to the remote application restricts the possible operation in the SIM.

Advantageously, said subscriber identity module has an input/output line and receives local commands belonging to a local application in said mobile station on said input/output line.

Said remote commands included in the first field of said enhanced message are virtually the same as said local command received by the input/output line.

In this way, the SIM can manage two kinds of commands, that is, local command and remote command without the necessity of duplicating the executable codes of the SIM (in general, the codes in ROM and/or EEPROM).

The present invention also provides a method for synchronizing and ensuring security of enhanced messages exchanged between a message service center and a mobile station (MS) of a cellular radio communication system, wherein each enhanced message has a header and a main

body, and said main body particularly has a first field for storing the remote commands pertaining to a remote application of the aforementioned mobile station.

Said mobile station is constituted with a terminal cooperating with a subscriber identity module. Said terminal has a means for receiving said enhanced message. Said subscriber identity module has a means for storing and processing the received enhanced message, and said subscriber identity module has a means for executing said remote commands to support said remote application.

Said method is characterized by particularly having the following steps:

• said message service center sends an enhanced message that also has a second field storing the current value of a synchronization counter in the main body to said mobile station;

• the subscriber identity module of the mobile station compares the current value of the synchronization counter included in said enhanced message with the previous value of the synchronization counter stored in the subscriber identity module;

• the subscriber identity module accepts or rejects said enhanced message depending on the result of comparing the current value with the previous value of the synchronization counter;

• the subscriber identity module updates said previous value by said current value if the enhanced message is accepted.

Preferably, the current value of the synchronization counter is incremented by a certain amount for each new enhanced message of said remote application transmitted by said message service center.

Also, said enhanced message is accepted by the subscriber identity module only when the current value of said synchronization counter is larger than said previous value.

In other words, in order to prevent replay of a message, the newest current value must be larger than the value included in the last accepted message (that is, the previous value sorted in the SIM).

Preferably, said step of updating the previous value of the synchronization counter by the current value is carried out only when the difference between the current value and the previous value is smaller than a prescribed maximum incrementation.

In this way, the counter can be prevented from being locked at its maximum value too quickly. In other words, the service life of the counter is extended, and the attack of quickly locking the SIM with the counter reaching its maximum value can be prevented. This is because the counter cannot be reset by the remote application when it is locked this way. Since this problem can only be solved by an administrator procedure, it will lead to additional cost.

Advantageously, the aforementioned method also has the following step:

• if said enhanced message is rejected by the subscriber identity module, the subscriber identity module will send an enhanced message including a specific error code that can notify the

message service center of the fact that the enhanced message it just transmitted has been rejected due to the synchronization problem of the counter to the message service center.

This is applicable particularly to the case when two consecutive messages with current values of the synchronization counter of N and N+1 are not received in their transmission order. In fact, since the second message is rejected (to be explained later) when the first received message is accepted, it is advantageous to notify the sender of the rejection reason, that is, the synchronization problem.

It can be understood that when the SIM receives the first message (value N+1), the previous value stored in the module is N-1. Therefore, the current value of the first message equal to N+1 is larger than said value N-1. Then, the previous value is updated by the current value of the first message. Consequently, when the SIM receives the second message, the previous value stored in the module is N+1. Consequently, the current value of the second message equal to N is smaller than the previous value N+1, and the second message is rejected because of the synchronization problem.

Advantageously, the main body of said enhanced message transmitted by the message service center to the mobile station also has a third field storing a first piece of locating information indicating the location in said data storage means where said previous value of the synchronization counter is stored.

The following steps are carried out before the subscriber identity module compares the current value and the previous value of the synchronization counter:

• the subscriber identity module reads the first piece of locating information stored in the third field of said enhanced message;

• the subscriber identity module deduces the previous value of the synchronization counter from the piece of locating information;

• the subscriber identity module reads the previous value of the synchronization counter stored at the aforementioned location.

In an embodiment of the present invention, said enhanced message transmitted by the message service center to the mobile station also has a fourth field storing a ciphertext known as transmitted ciphertext calculated by at least partially using the content of the second field storing the current value of the synchronization counter.

The aforementioned process also has the following steps:

• the subscriber identity module at least partially uses the content of the second field in said enhanced message to calculate a local ciphertext;

• the subscriber identity module compares said transmitted ciphertext with said local ciphertext such that said enhanced message is accepted if the transmitted ciphertext is the same as the local ciphertext and is rejected otherwise.

Advantageously, said subscriber identity module stores a cryptographic function and an associated key specific to said remote application in the data storage means of the subscriber identity module to calculate said local ciphertext.

Said enhanced message transmitted by the message service center to the mobile station also has a fifth field storing a third piece of locating information indicating the location in said data storage means where said cryptographic function and said associated key specific to said remote application are stored.

The aforementioned step of calculating the local ciphertext by the subscriber identity module has the following steps:

• the subscriber identity module reads said third piece of locating information stored in the fifth field of said enhanced message;

• the subscriber identity module deduces the storage locations of said cryptographic function and said associated key from the piece of locating information;

• the subscriber identity module uses said cryptographic function and said associated key as well as at least part of the content of the second field in said enhanced message to calculate said local ciphertext.

In an advantageous embodiment of the present invention wherein the data storage means of the subscriber identity module has a hierarchical structure of at least three levels and having at least the following three kinds of files:

• master file, or primary directory;

• dedicated file or secondary directory located under said master file;

• elementary file located under said dedicated file known as parent dedicated file or directly located under said master file known as parent master file,

said method is characterized by the following facts: an elementary system file (EF SMS System) suitable for said remote application has a second piece of locating information indicating the location in the data storage means of the subscriber identity module where said previous value of the synchronization counter is stored;

said third field also constitutes said fifth field, and said first piece of locating information also constitutes said third piece of locating information; and

the first piece of locating information stored in said third field is an identifier for dedicated file (DF) or master file (MF) related to said elementary system file (EF SMS System) depending on a predetermined search strategy in the data storage means.

Advantageously, the main body of said enhanced message transmitted by the message service center to the mobile station also has a sixth field storing a checksum known as a transmitted checksum, the calculation of which at least partially includes the content of the first field (3) storing remote commands.

Said method also has the following steps:

• the subscriber identity module uses at least part of the content of the first field in said enhanced message to calculate a local checksum;

• the subscriber identity module compares said transmitted checksum with said local checksum such that said enhanced message is accepted if said transmitted checksum is the same as the local checksum and is rejected otherwise.

Other characteristics and merits of the present invention can be understood by reading the following explanation of the preferable embodiments of the present invention provided as nonlimiting examples with reference to the attached figures.

• Figure 1 shows a specific embodiment of the enhanced message structure disclosed in the present invention.

• Figures 2-4 show examples of exchanging enhanced messages with security by using the method of the present invention.

• Figure 5 shows an example of calculating the ciphertext used in the method of the present invention.

• Figure 6 shows a simple flow chart of a specific embodiment of the method disclosed in the present invention.

• Figures 7-9 show the details of the steps in the flow chart shown in Figure 6.

The present invention pertains to a particular enhanced message structure and to a method for synchronizing and ensuring the security of exchanging the enhanced messages having said structure.

In a specific embodiment to be explained below as a nonlimiting example, the cellular radio communication system is of the GSM type and uses enhanced short message service "ESMS").

Of course, the present invention is not limited to the GSM system but can be applied to all cellular radio communication systems that provide enhanced message service.

Conventionally, in the case of GSM, enhanced short messages are exchanged between a short message service center (SMS-C) and one or a plurality of mobile stations (MS). Each mobile station is constituted with a terminal cooperating with a subscriber identity module (SIM). The terminal has an enhanced message reception means. The SIM is equipped with means for storing and processing the received enhanced messages. Each enhanced message has remote commands belonging to a remote application of the SIM. The SIM is equipped with a means for executing these remote commands to support said remote application (possibly others).

Figure 1 shows a specific embodiment of the enhanced message structure disclosed in the present invention.

Conventionally, an enhanced message has a header 1 and a main body 2 (or TP-UD, "transfer layer protocol-user data"). Main body 2 particularly has a "command" field 3 storing remote commands.

According to the present invention, the objects of the commands are the conventional (operation or management) commands defined in GSM11.11, ISO78.16-4 or EN726-3, such as SELECT, UPDATE BINARY, UPDATE RECORD, SEEK, CREATE FILE, CREATERECORD, EXTEND, and the like. In other words, the format of these remote commands is the same as the local commands received by the input/output line of the SIM. Consequently, the SIM can process the remote commands in the same way as the local commands.

In the embodiment shown in Figure 1, the main body 2 of the enhanced message in the present invention also has "synchronization counter" field 4, "system" field 5, "SMS certificate" field 6, and "SMS-ID" field 7.

In the following, the main body 2 of the enhanced message and the contents of fields 4-7 will be explained in detail.

"Synchronization counter" field 4 stores the current value of the synchronization counter. As to be explained in detail based on Figures 2-4, 6, 8, the current value of the synchronization counter is compared with the previous value of the same synchronization counter stored in the data storage means of the SIM. The enhanced message is accepted or rejected by the SIM depending on the comparison result.

"System" field 5 stores the piece of locating information of a system file in the data storage means of the SIM, with the system itself directly including the elements suitable for the message sending remote application or other locating information of said elements in the data storage means of the SIM.

The elements suitable for sending the remote application refer to the previous value of the synchronization counter as well as a cryptographic function and its associated key (the last two elements can be used to calculate the "local" ciphertext compared with the "transmitted" ciphertext stored in "SMS certificate" field 6).

It is well known that the subscriber identity module having a hierarchical structure of at least three levels can be provided to the SIM, with at least the following three kinds of files:

- master file (MF), or primary directory;
- dedicated file (DF) or secondary directory located under said master file;
- elementary file (EF) located under said dedicated file known as parent dedicated file or directly located under said master file known as parent master file.

In the case of this hierarchical structure, said system file of the present invention is, for example, an elementary system file (EF SMS system). In this case, the piece of locating

information stored in "system" field 5 is an identifier ("input DF") for dedicated file (DF) or master file (MF) related to said elementary system file (EF SMS System) depending on a predetermined search strategy in the data storage means.

For example, the SIM can use an upstream retrieval mechanism (of the "backtracking" type) comprised of the following steps:

• first, retrieving the elementary system file under the dedicated file or the current master file (that is, the file indicated by the "input DF" identifier";

• then, if there is no elementary system file under the dedicated file or the current master file and the "input DF" identifier does not indicate the master file, retrieving the elementary file directly under the master file.

In this way, the SIM reads the "input DF" identifier included in "system" field 5 into the enhanced message. The elementary system file linked to the message sending remote application can be found from said "input DF" identifier. In said elementary file, for example, the SIM reads the following:

• directly, the current value of the synchronization counter; and

• the identifier of a dedicated file under which EF key_op including a pair (cryptographic function, associated key) associated with the message sending remote application is present.

"SMS certificate" field 6 stores ciphertext (referred to as "transmitted ciphertext" hereinafter). As to be explained in detail based on Figures 6 and 9, said transmitted ciphertext is compared with a local ciphertext calculated separately by the SIM. The enhanced message is accepted or rejected by the SIM depending on the comparison result.

In the following, an embodiment of calculating the SMS-Cert transmitted ciphertext (this calculation is, of course, the same as that for the local ciphertext) will be introduced. One has the following relationship:

SMS-Cert = the least significant four bytes of [$MAC\_Alg_{algo\_id}$(Kappli, SMS_data)], wherein

• [Alg_{algo_id}] is an algorithm associated with the remote application (this algorithm can be located by the elementary system file (EF SMS System) to which said remote application belongs);

• K_{appli} is a secret (or public) key associated with algorithm Alg_{algo_id};

• "SMS_data" = Sync ‖ application message, wherein

* "‖" represents the concatenation operator;

* "Sync" is the value of the synchronization counter (current value in the case of calculating the transmitted ciphertext);

* "Application message" is the content of "command" field 3 (storing the remote commands);

• MAC_Alg_{algo_id} is a function based on $Alg_{algo\text{-}id}$ that uses key K_{appli} to realize "MAC" type ("message authentication code") calculation with respect to the SMS_data concatenation.

Figure 5 shows an example of calculating SMS-Cert transmitted ciphertexts when algorithm Alg_{algo_id} is MoU A3A8. Of course, however, algorithm A3A8 is only an application example. It is also possible to use other algorithms. In particular, the algorithm used is specified (by algorithm identifier) for specific applications during implementation in more fields.

SMS_data concatenation is divided in n blocks B_1, B_2,.., B_{n-1}, B_n with $n \leq 9$. Blocks B_1-B_n, for example, have 16 bytes.

When the last block Bn having 16 bytes in SMS_data concatenation is not obtained, the last block is shifted to the left, and the right side is made up by the bytes with value 0 to form a block having 16 bytes known as B'_n. These blocks are included in the following calculation:

$$I_1 = A3A8\ (K_{appli},\ B_1)$$

$$R_2 = XOR\ (I_1,\ B_2)$$

$$I_2 = A3A8\ (K_{appli},\ R_2)$$

...

$$R_{n-1} = XOR\ (I_{n-2},\ B_{n-1})$$

$$I_{n-1} = A3A8\ (K_{appli},\ R_{n-1})$$

$$R_n = XOR\ (I_{n-1},\ B'_n)$$

$$I_n = A3A8\ (K_{appli},\ R_n)$$

I_n is the result of function MAC_A3A8. XOR is an operator that realizes "exclusive-OR" in bit unit between two chains of 16 bytes.

"SMS-Id" field 7 includes the checksum (referred to as "transmitted checksum" hereinafter). As to be explained more accurately below based on Figures 6 and 7, said transmitted checksum is compared with a local checksum calculated separately by the SIM. The enhanced message is accepted or rejected by the SIM depending on the comparison result.

In the following, an embodiment of calculating the SMS-Id transmitted checksum (this calculation is, of course, the same as that for the local checksum) will be introduced. One has the following relationship: SMS_Id = NON("ΣByte of "command" field 3).

Figure 6 shows the simple flow chart of a specific embodiment disclosed in the present invention for synchronizing and ensuring the security of exchanging enhanced messages having the structure shown in Figure 1.

In this embodiment, the method of the present invention particularly has the following steps:

• The message service center sends an enhanced message to the SIM of a mobile station (61).

• The SIM checks the transmitted checksum included in "SMS-Id" field 7 of the enhanced message (62).

• If the result of checking the transmitted checksum is incorrect (63), the SIM rejects the enhanced message. Otherwise (64), the SIM checks the current value of the synchronization counter included in "synchronization counter" field 4 (65).

• If the result of checking the current value of the synchronization counter is incorrect (66), the SIM rejects the enhanced message. Otherwise (67), the SIM immediately updates the previous value of the synchronization counter by the current value before conducting any other checks. Then, it checks the transmitted ciphertext included in "SMS certificate" field 6 (68).

• If the result of checking the transmitted ciphertext is incorrect (69), the SIM rejects the enhanced message. Other wise (610), the SIM executes the remote commands included in "command" field 3 (611).

As shown in detail in Figure 7, the step of checking transmitted checksum (62) has the following steps:

• The SIM reads the transmitted checksum in "SMS-Id" field 7 of the enhanced message (71).

• The SIM calculates the local checksum by following the same calculation principle as that used for calculating the transmitted checksum (72).

• The SIM compares the transmitted checksum with the local checksum (73).

In this way, in the first stage of verification, the enhanced message is accepted (64) if the transmitted checksum is the same as the local checksum. Otherwise, the enhanced message is rejected (63).

As shown in detail in Figure 8, the step of checking the current value of the synchronization counter (65) has the following steps:

• The SIM reads the current value of the synchronization counter in "synchronization counter" field 4 (81).

• The SIM reads the piece of locating information of the system file (EF SMS System) in "system" field 5 of the enhanced message (82). As explained above, this piece of locating information is the "input DF" identifier of the dedicated file (DF) or master file (MF) associated with the elementary system file (EF SMS System).

• The SIM deduces the location of the system file (EF SMS System) including the previous value of the synchronization counter in the data storage means of the SIM from said piece of locating information (83).

• The SIM reads the previous value of the synchronization counter in the system file (EF SMS System) (84).

• The SIM compares the current value of the synchronization counter with the previous value stored in the SIM (85).

• In this second stage of verification, if the current value is definitely larger than the previous value of the synchronization counter (67), the SIM will accept the enhanced message. Then, the SIM will update the previous value with the current value (86).

• If the current value is equal to or smaller than the previous value of the synchronization counter (66), the SIM will reject the enhanced message. In this case, the SIM can return an enhanced message including a specific code to the message service center to notify the message service center that the enhanced message that it has just sent was rejected due to synchronization problem of the counter (87).

For example, it is possible to decide to increase the current value of the synchronization counter by a prescribed amount (for example, equal to 1) for each enhanced message newly sent by the message service center. In this case, the enhanced message is accepted by the SIM only when the current value of the synchronization counter included in the enhanced message is larger than the previous value stored in the SIM.

The step 86 of updating the previous value of the synchronization counter by the current value can also be carried out only when the difference between the current value and the previous value of the synchronization counter is smaller than a prescribed maximum increment.

Figures 2-4 show different examples of exchanging enhanced messages with security according to the present invention. Each of these figures shows the variation in the current value of the synchronization counter represented by E_Sync (in "outside", on the left) and the variation in the stored value represented by S_Sync (in the SIM on the right). Each arrow represents a message.

In the first case (see Figure 2), synchronization and transmission of enhanced message are correct. In this case, E_Sync (=1) > S_Sync (=0). The previous value is updated to 1, and the remote commands are executed.

In the second case (see Figure 3), a problem occurs during transmission of an enhanced message. The SIM does not respond. On the other hand, the second transmission attempt is successful free of problem. Finally, E_Sync (=3) > S_Sync (=1). The previous value is updated to 3, and the remote commands are executed.

In the third case (see Figure 4), a synchronization problem occurs at the beginning. In fact, E_Sync (=1) < S_Sync (=5). A plurality of enhanced messages including the current value incremented sequentially are transmitted until the message service center is resynchronized with

the SIM. This is the case in which E_Sync (=6) > S_Sync (=5). In this case, the previous value is updated to 6, and the remote commands are executed.

As shown in detail in Figure 9, the process of checking the transmitted ciphertext (68) includes the following different steps:

• The SIM reads the current value of the synchronization counter in "SMS certificate" field 6 (91).

• The SIM calculates the local ciphertext by following the same calculation principle as that used for calculating the transmitted ciphertext (92).

• The SIM compares the transmitted ciphertext with the local ciphertext (93).

In this way, in the third stage of verification, the enhanced message is accepted if the transmitted ciphertext is the same as the local ciphertext (610). Otherwise, the enhanced message is rejected (69).

As shown in detail in Figure 9, the step of calculating the local ciphertext 92 has the following steps:

• The SIM reads the piece of locating information of the system file (EF SMS System) in the "system" field 5 of the enhanced message (94).

• The SIM deduces the location of the system file (EF SMS System) in the data storage means of the SIM from the piece of locating information (95). The system file itself includes other locating information that enables the SIM to find the cryptographic function linked with the enhanced message sending remote application and its associated key.

• The SIM uses the cryptographic function and its associated key to calculate the local ciphertext as described above (96).

In this case, the step 94 and the beginning of the step 95 have actually already been carried out in order to find the previous value of the synchronization counter (it is directly stored in the system file (EF SMS System)) as explained above.

Certainly, the present invention can be embodied in many other ways.

For example, it is also possible to have two different system files in order to find the previous value of the synchronization counter and the cryptographic function and its associated key. In this case, there are two "system" fields represented by symbol 5.

It is also possible to use a public key type cryptographic function.

Finally, the step of checking the checksum 62 can be omitted in some cases in the same way as the step of checking the ciphertext 68.

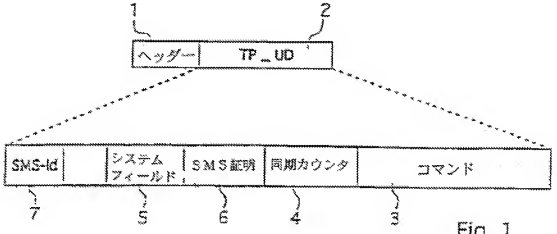

Fig. 1

Key: 1 Header
3 Command
4 Synchronization counter
5 System field
6 SMS certificate

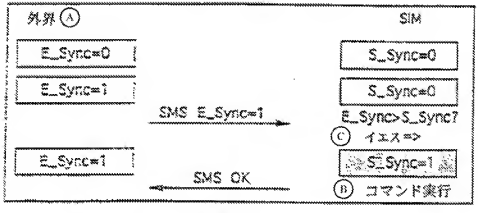

Fig. 2

Key: A Outside
B Execute command
C Yes

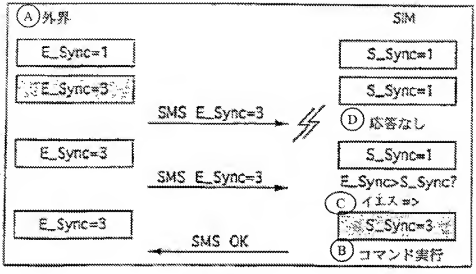

Fig. 3

Key:
- A Outside
- B Execute command
- C Yes
- D No response

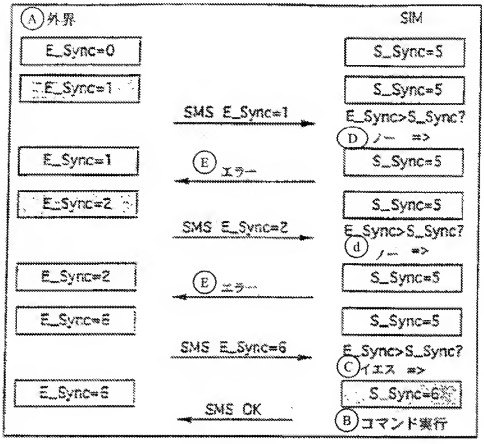

Fig. 4

Key: A Outside
B Execute command
C Yes
D No
E Error

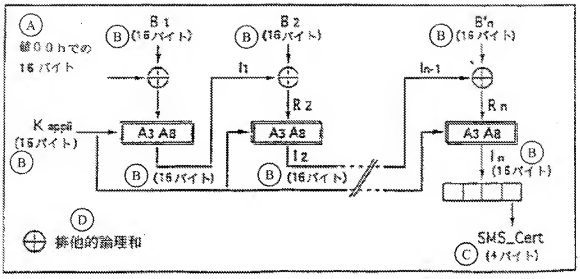

Fig. 5

Key: A 16 bytes with value 00h
B (16 bytes)
C (4 bytes)
D Exclusive-OR

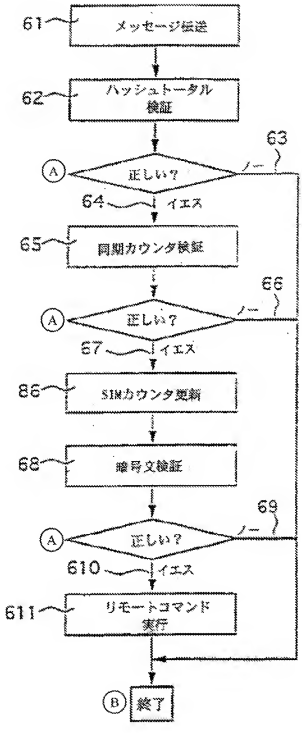
61
メッセージ伝送
62
ハッシュトータル
検証
63
A
正しい？
ノー
64
イエス
65
同期カウンタ検証
66
A
正しい？
ノー
67
イエス
86
SIMカウンタ更新
68
暗号文検証
69
A
正しい？
ノー
610
イエス
611
リモートコマンド
実行
B
終了

Fig. 6

Key: A Correct?
B End
61 Send message
62 Check the checksum
63 No
64 Yes
65 Check the synchronization counter
66 No
67 Yes
86 Update the SIM counter
68 Check the ciphertext
69 No
610 Yes
611 Execute remote command

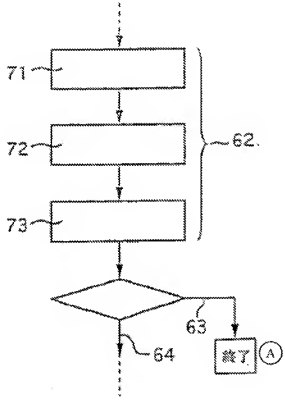

Fig. 7

Key: A End

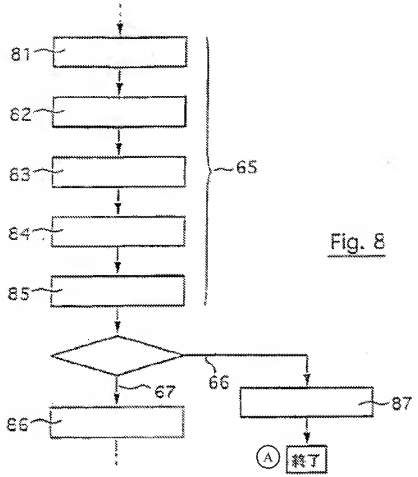

Fig. 8

Key: A End

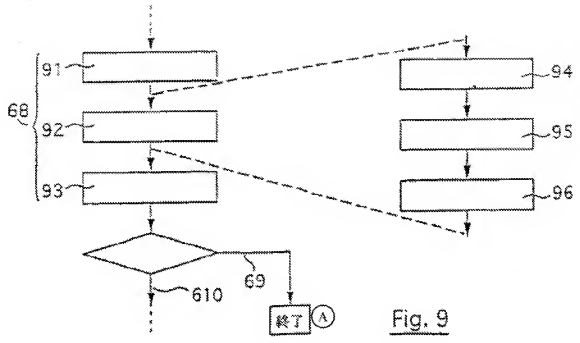

Fig. 9

Key: A End

Continued from front page
(72) Inventor: Cedric Huet
17 Avenue de Maréchal Joffre, La Ciotat, F-13600 France